

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE  
PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A secure pin entry device comprising:  
a microprocessor,  
memory,  
secure memory,  
identification information,  
a communication capability,  
encryption software,  
an activation program for completing a digital  
communication with an authorizing institute using said  
communication capability,  
said secure pin entry device including:  
a public encryption key stored in said memory,  
a private encryption key stored in said secure  
memory and a digital certificate which includes therein the  
public key and said identification information of said  
secure pin entry device.
2. A secure pin entry device as claimed in claim 1  
wherein said activation program includes a communication  
address to initiate a communication with the authorizing  
institute.
3. A secure pin entry device as claimed in claim 1  
wherein said secure pin entry device is ready for loading  
of financial keys and software from the authorizing  
institute using said encryption software and said public  
and private keys.
4. A secure pin entry device as claimed in claim 1  
includes:  
a connection port for an electronic cash register  
system which forms part of said communication capability.

5. A secure pin entry device as claimed in claim 1 wherein said activation program includes information specific to a predetermined authorizing institute which the device will communicate with.

6. A secure pin entry device as claimed in claim 1 wherein said device activation program is limited to a predetermined authorizing institute.

7. A method of downloading of confidential information or software from an authorizing institute to a secure pin entry device said method comprising:

providing said secure pin entry device with personal identification information including a serial number, a private key, a public key, and a digital certificate provided by a Certificate Authority having a public key and a private key and wherein said digital certificate includes the public key of said secure pin entry device,

locating said secure pin entry device in an operating location, forming a communication between said secure pin entry device and said authorizing institute and transmitting to said authorizing institute, said certificate;

said authorizing institute confirming said certificate using the public key of said Certificate Authority,

said secure pin entry device and said authorizing institute using said keys to encrypt and download confidential information received and deciphered by said secure pin entry device and used to program said secure pin entry device for secure communication with said authorizing institute.

8. A method as claimed in claim 7 wherein said secure pin entry device and said authorizing institute use said keys to form a shared secret, and said shared secret is

09582783.102201  
FOIA b7E b7C b7D

used to encrypt and decipher said confidential information used to program said secure pin entry device.

9. A method as claimed in claim 7 wherein the step of providing said secure pin entry device with said private key and said digital certificate occurs in a secure environment.

10. A method as claimed in claim 9 wherein said secure pin entry device is provided said private key and public key by an Initialization System and said Certificate Authority communicates with said Initialization System through a secure communication link.

11. A method as claimed in claim 10 including locating said Initialization System and said Certificate Authority in a common secure location.

12. A method as claimed in claim 10 wherein said Certificate Authority and said Initialization System exchange public keys initially, and thereafter communication using encryption based on said keys.

13. A method as claimed in claim 12 wherein the exchange of said public keys between said Certificate Authority and said Initialization System occurs only as required, and infrequently.

14. A method as claimed in claim 7 wherein said confidential information includes financial keys and/or software.

15. A method as claimed in claim 7 including providing said secure pin entry device with information specific to the authorizing institute prior to locating said device whereby the device is specific to the authorizing institute.

16. A method of customizing a financial transaction device having a unique identification for communication with a Financial Institute having a private key and a public key,

said method comprising providing said unique identification to an Initialization System;

having said Initialization System provide said financial transaction device with a private key and a public key, forwarding to a Certificate Authority the financial transaction device public key and unique identification; producing at the Certificate Authority a digital certificate for said financial transaction device;

providing said certificate to said financial transaction device; and

storing said certificate in said financial transaction device.

17. A method as claimed in claim 16 including having said Initialization System provide said transaction device with a communication address of said Financial Institute.

18. A method as claimed in claim 17 including having said Initialization System provide said financial transaction device with an initiation program used to initiate a communication with said Financial Institute using said communication address.